

WHEREAS, Provider, hereinafter referred to in this Exhibit as "Business Associate," acknowledges that the CDCR, hereinafter referred to in this Exhibit as "Covered Entity," has in its possession data that contains individual identifiable health information as defined by Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("HIPAA") and the regulations promulgated thereunder;

WHEREAS, Business Associate and Covered Entity acknowledge that the fulfillment of the Parties' obligations under this Service Agreement necessitates the exchange of, or access to, data including individual identifiable health information; and,

WHEREAS, the parties desire to comply with federal and California laws regarding the use and disclosure of individually identifiable health information, and in particular with the provisions of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations promulgated thereunder.

NOW, THEREFORE, in consideration of the mutual promises and covenants hereinafter contained, the Parties agree as follows:

#### **ARTICLE 1 DEFINITIONS**

Terms used, but not otherwise defined, in this Exhibit shall have the meanings set forth below.

- 1.1 "HHS Transaction Standard Regulation" means the Code of Federal Regulations ("CFR") at Title 45, Sections 160 and 162.
- 1.2 "Individual" means the subject of protected health information (PHI) or, if deceased, his or her personal representative.
- 1.3 "Parties" shall mean the Covered Entity and Business Associate. (Covered Entity and Business Associate, individually, may be referred to as a "Party".)
- 1.4 "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- 1.5 "PHI" shall have the same meaning as the term "protected health information" in 45 CFR §164.501, limited to the information created or received by Business Associate from or on behalf of the Covered Entity.
- 1.6 "Required By Law" shall have the same meaning as "required by law" in 45 CFR §164.501.
- 1.7 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Any other terms used, but not otherwise defined, in this Exhibit shall have the same meaning as those terms in the Privacy Rule.

**ARTICLE 2**  
**CONFIDENTIALITY**

2.1 Obligations and Activities of Business Associate. Business Associate agrees as follows:

- (a) not to use or further disclose PHI other than as permitted or required by this Agreement or as Required By Law;
- (b) to establish, maintain, and use appropriate safeguards to prevent use or disclosure of the PHI other than as permitted herein;
- (c) to report to Covered Entity any use, access or disclosure of the PHI not provided for by this Agreement, or any misuse of the PHI, including but not limited to systems compromises of which it becomes aware and to mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result thereof. Business Associate shall be responsible for any and all costs (including the costs of Covered Entity) associated with mitigating or remedying any violation of this Agreement;
- (d) to enforce and maintain appropriate policies, procedures, and access control mechanisms to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. The access and privileges granted to any such agent shall be the minimum necessary to perform the assigned functions;
- (e) to provide access, at the request of Covered Entity, and in the time and manner reasonable designated by Covered Entity, to PHI in a Designated Record Set (as defined in the Privacy Rule), to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524;
- (f) to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of Covered Entity or an Individual, and in the time and manner reasonably requested by Covered Entity.
- (g) to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner reasonably requested by Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- (h) to document such disclosures of PHI, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528. Said documentation shall include, but not be limited to, the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure. Said documentation shall be made available to Covered Entity upon request.

- (i) to provide to Covered Entity or an Individual, in a time and manner reasonably requested by Covered Entity, information collected in accordance with Section 2.1(h) above to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528.
- (j) to promptly notify Covered Entity of all actual or suspected instances of deliberate unauthorized attempts (both successful and unsuccessful) to access PHI. Such notice shall be made to Covered Entity by telephone as soon as Business Associate becomes aware of the unauthorized attempt, and this telephone notification shall be followed within two (2) calendar days of the discovery of the unauthorized attempt by a written report to Covered Entity from Business Associate. Business Associate shall, at the same time, report to Covered Entity any remedial action taken, or proposed to be taken, with respect to such unauthorized attempt. Covered Entity shall have the discretion to determine whether or not any such remedial action is sufficient, and all such remedial action shall be at Business Associate's expense.
- (k) to maintain and enforce policies, procedures and processes to protect physical access to hardware, software and/or media containing PHI (e.g., hardcopy, tapes, removable media, etc. ) against unauthorized physical access during use, storage, transportation, disposition and /or destruction.
- (l) to ensure that access controls in place to protect PHI and processing resources from unauthorized access are controlled by two-factor identification and authentication: a user ID and a Token, Password or Biometrics.
- (m) to implement, use and monitor its compliance with appropriate technological, administrative and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement. Business Associate shall provide Covered Entity with evidence of such safeguards upon Covered Entities request. Covered Entity has the right to determine, in its sole discretion, whether such safeguards are appropriate, and to require any additional safeguards it deems necessary.
- (n) In the event that Business Associate is served with legal process (e.g. a subpoena) or request from a governmental agency (e.g. the Secretary) that potentially could require the disclosure of PHI, Business Associate shall provide prompt (i.e., within twenty-four (24) hours) written notice of such legal process (including a copy of the legal process served) to the designated person at the Covered Entity. In addition, Business Associate shall not disclose the PHI without the consent of Covered Entity unless pursuant to a valid and specific court order or to comply with a requirement for review of documents by a governmental regulatory agency under its statutory or regulatory authority to regulate the activities of either party.
- (o) to submit to periodic audits by Covered Entity verifying Business Associate's compliance with appropriate technological, administrative and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement, as well as compliance with the terms and conditions pursuant to this Agreement and compliance with state and federal laws and regulations. Audit review may be undertaken directly by the Covered Entity or by third parties

engaged by the Covered Entity. Business Associate shall cooperate fully with Covered Entity or any such third party in connection with such audits.

2.2 Disclosures Required By Law.

In the event that Business Associate is required by law to disclose PHI, Business Associate will immediately provide Covered Entity with written notice and provide Covered Entity an opportunity to oppose any request for such PHI or to take whatever action Covered Entity deems appropriate.

2.3 Specific Use and Disclosure Provisions.

- (a) Except as otherwise limited in this Agreement, Business Associate may use PHI only to carry out the legal responsibilities of the Business Associate under this Service Agreement.
- (b) Except as otherwise limited in this Agreement, Business Associate may only disclose PHI (i) as Required By Law, or (ii) in the fulfillment of its obligations under the Service Agreement and provided that Business Associate has first obtained (A) the consent of Covered Entity for such disclosure, (B) reasonable assurances from the person to whom the information is disclosed that the PHI will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and (C) reasonable assurances from the person to whom the information is disclosed that such person will notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.4 Obligations of Covered Entity.

- (a) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosures of PHI.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- (d) For any PHI received by Covered Entity from Business Associate on behalf of a third party or another covered entity, Covered Entity agrees to be bound to the obligations and activities of Business Associate enumerated in Section 2.1 as if and to the same extent Covered Entity was the named Business Associate hereunder.

**2.5 Permissible Requests by Covered Entity.**

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

**2.6 Policy and Procedure Review.**

Upon request, Business Associate shall make available to Covered Entity any and all documentation relevant to the safeguarding of PHI including but not limited to current policies and procedures, operational manuals and/or instructions, and/or employment and/or third party agreements.

**ARTICLE 3  
SECURITY****3.1 Government Healthcare Program Representations.**

Business Associate hereby represents and warrants to Covered Entity, its shareholders, members, directors, officers, agents, or employees have not been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or state healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or state law (including without limitation a plea of nolo contendere or participation in a first offender deterred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under a federal or state healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in part by any federal, state or local government agency, (d) the unlawful, manufacture, distribution, prescription, or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. Business Associate further agrees to notify Covered Entity immediately after Business Associate becomes aware that the foregoing representation and warranty may be inaccurate or may be incorrect.

**3.2 Security Procedures.**

Each Party shall employ security procedures that comply with HIPAA and all other applicable state and federal laws and regulations (collectively, the "Law") and that are commercially reasonable, to ensure that transactions, notices, and other information that are electronically created, communicated, processed, stored, retained or retrieved are authentic, accurate, reliable, complete and confidential. Moreover, each Party shall, and shall require any agent or subcontractor involved in the electronic exchange of data to:

- (a) require its agents and subcontractors to provide security for all data that is electronically exchanged between Covered Entity and Business Associate;
- (b) provide, utilize, and maintain equipment, software, services and testing necessary to assure the secure and reliable transmission and receipt of data containing PHI;
- (c) maintain and enforce security management policies and procedures and utilize mechanisms and processes to prevent, detect, record, analyze, contain and resolve unauthorized access attempts to PHI or processing resources;
- (d) maintain and enforce policies and guidelines for workstation use that delineate appropriate use of workstations to maximize the security of data containing PHI;

- (e) maintain and enforce policies, procedures and a formal program for periodically reviewing its processing infrastructure for potential security vulnerabilities;
- (f) implement and maintain, and require its agents and subcontractors to implement and maintain, appropriate and effective administrative, technical and physical safeguards to protect the security, integrity and confidentiality of data electronically exchanged between Business Associate and Covered Entity, including access to data as provided herein. Each Party and its agents and subcontractors shall keep all security measures current and shall document its security measures implemented in written policies, procedures or guidelines, which it will provide to the other Party upon the other Party's request.

**ARTICLE 4**  
**EXCHANGE OF STANDARD TRANSMISSIONS**

4.1 Obligations of the Parties. Each of the Parties agrees that for the PHI,

- (a) it will not change any definition, data condition or use of a data element or segment as proscribed in the HHS Transaction Standard Regulation.
- (b) it will not add any data elements or segments to the maximum denied data set as proscribed in the HHS Transaction Standard Regulation.
- (c) it will not use any code or data elements that are either marked "not used" in the HHS Standard's implementation specifications or are not in the HHS Transaction Standard's implementation specifications.
- (d) it will not change the meaning or intent of any of the HHS Transaction Standard's implementation specifications.

4.2 Incorporation of Modifications to HHS Transaction Standards.

Each of the Parties agrees and understands that from time-to-time, HHS may modify and set compliance dates for the HHS Transaction Standards. Each of the Parties agrees to incorporate by reference into this Agreement any such modifications or changes.

4.3 Code Set Retention.

If applicable, both parties understand and agree to keep open code sets being processed or used in this Agreement for at least the current billing period or any appeal period, which ever is longer.

4.4 Business Associate Obligations.

- (a) Business Associate shall not submit duplicate transmissions unless so requested by Covered Entity.
- (b) Business Associate shall only perform those transactions, which are authorized by Covered Entity. Furthermore, Business Associate assumes all liability for any damage, whether direct or indirect, to the electronic data or to Covered Entity's systems caused by Business Associate's unauthorized use of such transactions.
- (c) Business Associate shall hold Covered Entity harmless from any claim, loss or damage of any kind, whether direct or indirect, whether to person or property, arising out of or related to (1) Business Associate's use or unauthorized disclosure of the electronic data; or (2) Business Associate's submission of data, including but not limited to the submission of incorrect, misleading, incomplete or fraudulent data.



- (d) Business Associate agrees to maintain adequate back-up files to recreate transmissions in the event that such recreations become necessary. Back-up tapes shall be subject to this Agreement to the same extent as original data.
- (e) Business Associate agrees to trace lost or indecipherable transmissions and make reasonable efforts to locate and translate the same. Business Associate shall bear all costs associated with the recreation of incomplete, lost or indecipherable transmissions if such loss is the result of an act or omission of Business Associate.
- (f) Business Associate shall maintain, for seven (7) years, true copies of any source documents from which it produces electronic data.
- (g) Except encounter data furnished by Business Associate to Covered Entity, Business Associate shall not (other than to correct errors) modify any data to which it is granted access under this Agreement or derive new data from such existing data. Any modification of data is to be recorded, and a record of such modification is to be retained by Business Associate for a period of seven (7) years.
- (h) Business Associate shall not disclose security access codes to any third party in any manner without the express written consent of Covered Entity. Business Associate furthermore acknowledges that Covered Entity may change such codes at any time without notice. Business Associate shall assume responsibility for any damages arising from its disclosure of the security access codes or its failure to prevent any third party use of the system without the express written consent of Covered Entity.
- (i) Business Associate shall maintain general liability coverage, including coverage for general commercial liability, for a limit of not less than one million dollars, as well as other coverage as Covered Entity may require to compensate any parties damaged by Business Associate's negligence. Business Associate shall provide evidence of such coverage in the form of a certificate of insurance and agrees to notify Covered Entity and/or HOI immediately of any reduction or cancellation of such coverage.
- (j) Business Associate agrees to conduct testing with Covered Entity to ensure delivery of files that are HIPAA-AS Compliant and to accommodate Covered Entity's specific business requirements.

#### 4.5 Confidential And Proprietary Information

(a) Proprietary Information

Business Associate acknowledges that it will have access to certain proprietary information used in Covered Entity's business. Covered Entity's proprietary information derives its commercial value from the fact that it is not available to competitors or any third parties, and the disclosure of this information would or could impair Covered Entity's competitive position or otherwise prejudice its ongoing business. Business Associate agrees to treat as confidential, and shall

not use for its own commercial purpose or any other purpose, Covered Entity's proprietary information. Business Associate shall safeguard Covered Entity's proprietary information against disclosure except as may be expressly permitted herein. Such proprietary information includes, but is not limited to, confidential information concerning the business operations or practices of Covered Entity, including specific technology processes or capabilities.

**ARTICLE 5  
MISCELLANEOUS**

5.1 Indemnification.

Business Associate shall indemnify, defend, and save harmless the State, CDCR, and CDCR's officers, employees and agents, against any and all losses, liabilities, settlements, claims, demands, damages, or deficiencies (including interest) and expenses of any kind (including, but not limited to, attorneys' fees) arising out of or due to a breach of the terms of this Exhibit to the Service Agreement, and arising out of Business Associate's acts or omissions in regard to the terms of this Exhibit to the Service Agreement. The foregoing indemnity is in addition to any other save harmless or indemnification set forth in this entire Agreement.

5.2 Term and Termination.

- (a) Term. The Term of this Agreement shall be effective as of the first date of commencement of services under this entire agreement, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- (b) Termination for Cause. Upon a material breach by Business Associate of its obligation hereunder, Covered Entity may (i) terminate this Agreement and the Service Agreement; (ii) permit Business Associate to cure the breach; (iii) report the violation to the Secretary; and/or (iv) require Business Associate to take such other action as Covered Entity may request, at Business Associate's expense.

Covered Entity's remedies under this paragraph shall be cumulative, and the exercise of any remedy shall not preclude the exercise of any other. If Covered Entity elects to terminate the Agreement pursuant to a breach of terms and conditions of this Exhibit, Covered Entity shall be relieved of any further obligations under the entire Agreement, and shall be immediately entitled to a refund of any amounts prepaid from the date of the termination through the end of the payment period, on a pro rata basis.

The foregoing termination language is in addition to any other termination language set forth in the entire agreement.

## (c) Effect of Termination.

(i) Except as provided in paragraph 5.2(c)(ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

(ii) In the event that Business Associate determines that returning the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon Covered Entity's agreement that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

5.3 Disputes.HIPAA Appeal Procedures

CDCR has established and shall maintain an appeal procedure in accordance with CDCR Department Operations Manual, Section 22040.16. Business Associate agrees that disputes arising under the terms of this Exhibit shall be resolved in accordance with the following:

1. Verbal Appeal

Business Associate and CDCR's Privacy Officer, shall first attempt to resolve the problem by informal discussion. Business Associate agrees that CDCR's Division of Correctional Health Care Services shall be used as a resource in solving potential disputes.

2. Informal Appeal

If the issue is not resolved at the verbal appeal level, Business Associate shall file, within thirty (30) working days, an informal written appeal specifying: the issue(s) of dispute, legal authority or other basis for Business Associate's position, supporting evidence, and remedy sought, with the CDCR Chief, Licensing and Information Systems, and provide a photocopy to the CDCR Assistant Deputy Director, Office of Business Services. The CDCR Chief, Licensing and Information Systems, shall make a determination on the issue and respond in writing within thirty (30) working days of receipt of the informal appeal, indicating the decision reached.

3. Formal Appeal

Should Business Associate disagree with the informal appeal decision, Business Associate shall submit, within ten (10) working days after Business Associate's receipt of the decision of the informal appeal, to the CDCR Deputy Director, Division of Correctional Health Care Services, and a photo copy to the CDCR, Assistant Deputy Director, Office of Business Services, written notification indicating why the informal appeal decision is unacceptable, along with a copy of the original statement of dispute and a copy of CDCR's response. The CDCR Deputy Director, Division of

Correctional Health Care Services, or his/her designee may meet with Business Associate to review the issues within twenty (20) working days of the receipt of Business Associate's notification and shall provide Business Associate with written notification of the decision within forty-five (45) working days from the receipt of the formal appeal.

The foregoing dispute process is solely for the purpose of disputes arising from the terms and conditions of this Exhibit. Disputes in relation to the scope of work and other terms and conditions shall be in accordance with any other dispute language set forth in the entire Agreement.

5.4 Injunctive Relief.

Notwithstanding any rights or remedies provided for in Section 5.3, Covered Entity retains all rights to seek injunctive relief to prevent the unauthorized use of disclosure of PHI by Business Associate or any agent, contractor or third party that received PHI from Business Associate.

5.5 Regulatory References.

A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

5.6 Amendment.

The Parties agree to take such action as is necessary to amend this Agreement from time to time to the extent necessary for Covered Entity to comply with the requirements of HIPAA and its regulations. All amendments to this Exhibit shall be in writing and signed by both parties through a formal amendment to the entire agreement.

5.7 Survival.

The respective rights and obligations of Business Associate and Covered Entity under Sections 4.5, 5.1 and 5.2(c) of this Agreement shall survive the termination of this Agreement.

5.8 Limitation of Damages.

Other than liabilities under Section 5.1, neither party shall be liable to the other for any special, incidental, exemplary, punitive or consequential damages arising from or as a result of any delay, omission, or error in the electronic transmission or receipt of any information pursuant to this Agreement, even if the other Party has been advised of the possibility of such damages.

5.9 Interpretation.

Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

5.10 Third Party Beneficiary

Unless otherwise set forth herein, nothing contained herein is intended, nor shall it be construed, to create rights running of the benefit of third parties.

5.11 Notices

Any HIPAA related notice required hereunder shall be deemed to be sufficient if mailed to the parties at the addresses listed on original contract. In order to avoid unreasonable delay in the provision of the services to be rendered pursuant to this Agreement, Business Associate and Covered Entity shall each designate a specific "HIPAA" representative(s) for the purpose of communication between the parties. Such representative(s) may be changed upon written notice to the other party.

Covered Entity:

California Department of Corrections and Rehabilitation  
Privacy Officer  
HIPAA Compliance Unit  
Division of Correctional Health Care Services  
P.O. Box 942883  
Sacramento, CA 94283-0001

Telephone: (916) 327-1842  
Facsimile: (916) 327-0545